

REMARKS

This Amendment addresses the issues outstanding from the final Office Action dated June 14, 2006. Applicants respectfully request favorable reconsideration of this application, as amended.

Applicants thank the Examiner for indicating that Claims 15 and 16 are directed to allowable subject matter.

Claims 14-34 are pending. Claims 1-13 were previously cancelled without prejudice or disclaimer. By this Amendment, Claims 14, 16, 18, 21, 22, 28-30, 33 and 34 have been amended to more particularly recite certain distinctive features of Applicant's invention, as discussed below.

In the Office Action, Claims 14-34 were rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Furthermore, Claim 14 was rejected under 35 U.S.C. § 102(e) over U.S. Patent No. 6,304,658 B1 to Kocher ("Kocher"), and Claims 17-34 were rejected under 35 U.S.C. § 103 over Kocher in combination variously with Menezes, Stinson, Poore, and Liskov.

Regarding the rejection under § 101, it appears that the rejection is based at least in part on the "technological arts" test. Applicants respectfully submit that the "technological arts" test is no longer a proper ground for rejection. *See* OG Notice 22 November 2005, Annex III(a) (Improper Tests for Subject Matter Eligibility); *See also Ex parte Lundgren*, Appeal No. 2003-2088, p.9 (Bd. Pat. App. & Interferences, 2005) (holding "there is currently no judicially recognized separate 'technological arts' test to determine patent eligible subject matter under Sec. 101").

Further, and without acceding to the rejection under § 101, Claim 14 recites, *inter alia*, a method for verifying a signature, or respectively an authentication, utilizing an

asymmetric private-key (d) and public-key (e, n) cryptographic calculation process between a terminal having first computing means provided with a first computing capacity and a smart card comprising second computing means provided with second computing capacity lower than said first computing capacity, and . . . using said first computing means for calculating at the level of said terminal at least one prevalidation value representing at least a quotient of a modulo n calculation. Thus, Claim 14 is directed to a method that produces a beneficial real-world result, to wit, that the smart card can have a lower computing capacity than the terminal because the terminal first computing means is used to calculate at least one prevalidation value, resulting in the smart card having less calculations to perform. Therefore, Applicants respectfully submit that Claim 14 is directed to “a practical method . . . producing a beneficial result or effect,” and thus recites a concrete, useful and *tangible* result. *See Diamond v. Diehr*, 450 U.S. 175, 187 (1981).

For at least the foregoing reasons, Applicants respectfully request that this rejection be withdrawn.

Regarding the prior art rejections, without acceding to the rejections under §§ 102 and 103, Claims 14, 16, 18, 21, 22, 28-30, 33 and 34 have been amended to more particularly recite certain distinctive features of Applicant's invention. In particular, independent Claim 14 now recites, *inter alia*, a method for verifying a signature, or respectively an authentication, utilizing an asymmetric private-key (d) and public-key (e, n) cryptographic calculation process between a terminal having first computing means provided with a first computing capacity and a smart card comprising second computing means provided with second computing capacity lower than said first computing capacity, and . . . using said first computing means for calculating at the level of said terminal at

least one prevalidation value representing at least a quotient of a modulo n calculation. It is apparent the Kocher does not teach or suggest these features, nor do any of the secondary references.

In contrast, for example, Kocher teaches a decryption operation (or signing) comprising the following operations performed at the level of the smart card:

receiving the input message C by the modular exponentiator of the verifier (See Kocher, Fig. 3 and col. 17, lines 30-33);

blinding the obtained value by computing $C' \leftarrow (C)(B_i) \bmod n$ (See Kocher, col. 17, lines 32-40); and

computing the blinded result as M' (See Kocher, col. 17, line 45).

Kocher does not teach or suggest, at minimum, the Claim 14 feature of using first computing means of a terminal for calculating, at the level of the terminal, at least one prevalidation value representing at least a quotient of a modulo n calculation.

Moreover, Kocher does not teach or suggest the Claim 14 feature of the terminal transmitting to the smart card response data comprising at least the prevalidation value.

Accordingly, Applicants respectfully submit that Claim 14 distinguishes patentably from Kocher. None of the secondary references appear to overcome the deficiencies of Kocher.

Therefore, Applicants respectfully submit that this application is in condition for allowance. A prompt Notice of Allowance is respectfully solicited.


The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2146-906752) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

EJK:EGK

Miles & Stockbridge P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
(703) 903-9000

September __, 2006

Respectfully submitted,

By: 
Edward J. Kondracki
Reg. No. 20,604

Eric G. King
Reg. No. 42,736